



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: Virgil D. Gligor et al.

Title: BLOCK ENCRYPTION METHOD AND SCHEMES FOR DATA  
CONFIDENTIALITY AND INTEGRITY PROTECTION

Appl. No.: 09/761,771

Filing Date: 01/18/2001

Examiner: (unassigned)

Art Unit: 2131

**RECEIVED**  
AUG 23 2001  
Technology Center 2100

**PRELIMINARY AMENDMENT TRANSMITTAL**

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Transmitted herewith is Amendment A in the above-identified application.

☒ Small Entity status under 37 C.F.R. § 1.9 and § 1.27 has been established by a Small Entity statement previously submitted.

☐ Small Entity statement is enclosed.

☒ The fee required for additional claims is calculated below:

	Claims as Amended		Previously Paid For		Extra Claims Present		Rate		Additional Claims Fee
Total Claims:	82	—	64	=	18	x	\$18.00	=	\$324.00
Independents:	15	—	12	=	3	x	\$80.00	=	\$240.00
First presentation of any Multiple Dependent Claims:						+	\$270.00	=	\$0.00
CLAIMS FEE TOTAL:								=	\$564.00

☐ Applicant hereby petitions for an extension of time under 37 C.F.R. §1.136(a) for the total number of months checked below:

<input type="checkbox"/>	Extension for response filed within the first month:	\$110.00	\$0.00
<input type="checkbox"/>	Extension for response filed within the second month:	\$390.00	\$0.00
<input type="checkbox"/>	Extension for response filed within the third month:	\$890.00	\$0.00
<input type="checkbox"/>	Extension for response filed within the fourth month:	\$1,390.00	\$0.00
<input type="checkbox"/>	Extension for response filed within the fifth month:	\$1,890.00	\$0.00
EXTENSION FEE TOTAL:			\$0.00
CLAIMS AND EXTENSION FEE TOTAL:			\$564.00
<input checked="" type="checkbox"/>	Small Entity Fees Apply (subtract ½ of above):		\$282.00
TOTAL FEE:			\$282.00


- ☐ Please charge Deposit Account No. 19-0741 in the amount of \$282.00. A duplicate copy of this transmittal is enclosed.
- ☒ A check in the amount of \$282.00 is enclosed.
- ☒ The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

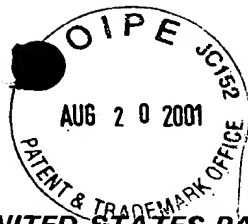
Please direct all correspondence to the undersigned attorney or agent at the address indicated below.

Respectfully submitted,

Date August 20, 2001

FOLEY & LARDNER  
 Washington Harbour  
 3000 K Street, N.W., Suite 500  
 Washington, D.C. 20007-5109  
 Telephone: (202) 672-5485  
 Facsimile: (202) 672-5399

By  34,371  
 for William T. Ellis  
 Attorney for Applicant  
 Registration No. 26,874



Atty. Dkt. No. 068398-0102

#3/a  
KWS  
9-5-01

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: Virgil D. Gligor et al.  
Title: BLOCK ENCRYPTION METHOD AND SCHEMES FOR DATA  
CONFIDENTIALITY AND INTEGRITY PROTECTION  
Appl. No.: 09/761,771  
Filing Date: 01/18/2001  
Examiner: Unassigned  
Art Unit: 2131

RECEIVED  
AUG 23 2001  
Technology Center 2100

**PRELIMINARY AMENDMENT**

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Prior to examination of the present application, Applicants respectfully request that the above-identified application be amended as follows:

Please add the following new claims:

**In the Claims:**

65. (New) An encryption method for providing both data confidentiality and integrity for a message, comprising the steps of:

receiving an input plaintext string comprising a message;

generating a plurality of equal-sized blocks of  $\ell$  bits in length from the input plaintext string;

creating an MDC block of  $\ell$  bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-sized blocks;

making one and only one processing pass with a single cryptographic primitive over each of said equal-sized blocks and the MDC block to create a plurality of hidden ciphertext blocks each of  $\ell$  bits in length; and

08/21/2001 MDANTE1 00000095 09761771

01 FC:203 162.00 OP  
02 FC:202 120.00 OP